Information Security Controls Overview

This document serves as an overview of some of the notable information security controls and practices we have in place to foster a culture of security to protect client's and our own data.

ANTIVIRUS SCANNERS, FIREWALL, & ENCRYPTION

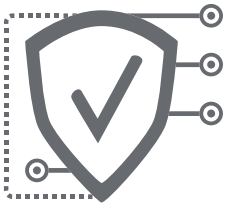
We protect our network and host environments with industry-accepted tools, including web application firewalls (WAF), network firewalls, intrusion detection/prevention systems (IDS/IPS), security information and event management software (SIEM), virus/malware detection software and data loss prevention (DLP) solutions. Sensitive client information is encrypted both during transmission and at rest using industry standard protocols.

End-users are protected using a host-based antivirus solution with daily updated virus signatures, real-time scanning and web proxy functionality to prevent the installation of adware, malware and spyware.

Additionally, all employee computers use full disk encryption technology to protect data-at-rest and offsite data backups are encrypted and transported via trusted courier in a sealed, locked case.

BUSINESS CONTINUITY & DISASTER RECOVERY

Continuity, availability and reliability of customer and company operations is critical to Paylocity and our clients. Paylocity follows best practices developed by the Disaster Recovery Institute and the Business Continuity Institute when creating, implementing, maintaining and monitoring its continuity deliverables, as testing of business continuity/ disaster recovery plans occurs at least annually.



Having a primary data center (IL) as well as a backup data center (WI), Paylocity relies on a multi-tiered, redundant backup strategy to help ensure recovery of archived data. Backup procedures include daily snapshots of all critical client data to multiple catalog stores. This includes both magnetic tape and local storage media, review of daily backup logs, full monthly backups and daily differential backups. Backups are tested regularly to ensure recovery reliability and backup tapes are encrypted at rest and securely transported to our secondary data center location.

CHANGE MANAGEMENT

Changes to our internal systems and applications are reviewed, approved and scheduled at weekly change management meetings, while emergency changes require senior executive approval.

DATA SECURITY & PRIVACY TRAINING

Paylocity provides training for employees on data security and privacy on a regular basis. This training is designed to educate our employees on safe handling of sensitive information, appropriate response to a suspected data security breach and awareness around responsibilities for security. Topics covered in this training include but are not limited to secure communication, approved methods for handling sensitive data, data disclosure policy, and employee responsibilities. Our employees must demonstrate understanding of company policy before completing the course.

EXTERNAL WEB APP PENETRATION TESTING

In addition to internal testing, Paylocity engages outside experts at least annually to perform penetration testing on our web applications used by our clients.

INFORMATION SECURITY POLICY DELIVERABLES

Paylocity maintains formal and documented information security policies. Our policies map to standard industry frameworks such as the National Institute of Standards and Technology (NIST), Committee of Sponsoring Organizations (COSO), and International Organization for Standardization (ISO) 27001 and 27002 to establish structured governance, policies, standards and controls. Policy deliverables are formally reviewed and approved by senior management on a periodic basis, as are policy updates and revisions.

INTERNAL WEB APP PENETRATION TESTING

Paylocity performs a comprehensive security assessment on all new web applications before and after release into production.

PHYSICAL & ENVIRONMENTAL SECURITY

Facilities owned or contracted by Paylocity employ physical protections to deter unauthorized access, protect systems and data, and monitor availability and environmental conditions. Such measures include surveillance cameras, keycard access, and physical security presence during non-business hours. Appropriate fire suppression, HVAC/environmental controls and power sources exist throughout Paylocity's facilities and are regularly tested and maintained to ensure performance.

PRIVACY LAW COMPLIANCE

Paylocity participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. Paylocity is committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable Principles.

Privacy Shield Framework

RISK MANAGEMENT

Paylocity has established an Information Security Steering Committee (ISSC) comprised of key executive and operating personnel to oversee the ongoing management of the organization's risks to information systems. This governance body reviews and approves policies and monitors the threat landscape, areas of vulnerability, and control design and efficacy. A risk assessment is conducted at minimum annually and reviewed by the ISSC, senior management and the Board of Directors.

SECURITY FOCUSED ROLES

Paylocity's deep commitment to security is reflected in the security-focused roles within the IT and Information Security departments as well as in the investments we make in keeping these critical employees updated on the latest security trends. These roles exist to monitor and improve the security of Paylocity products and to secure and protect client data from internal and external attacks.

The Information Security department invests in the team members through training and certifications from reputable organizations such as Information System Security Certification Consortium, Inc. (ISC2), the Information Systems Audit and Control Association (ISACA), EC-Council, and others. Members of the Information Security department and select IT management are Certified Information Systems Security Professionals (CISSPs).

Paylocity personnel also maintain relationships with special interest groups concerned with security, such as the Open Web Application Security Project (OWASP), the Information Systems Security Association (ISSA) and InfraGard.

SSAE 18 AUDIT

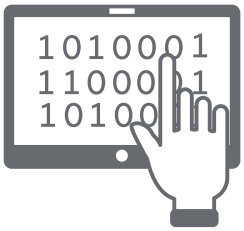
Paylocity uses a reputable independent accounting firm to perform an assessment of our procedures and controls as part of our annual SSAE 18 audit. Each control is tested and the results reviewed by senior management.

VULNERABILITY SCANNING & REMEDIATION

Paylocity employs two different strategies for vulnerability management. Vulnerability detection and patching on employee hardware are performed automatically on a daily basis. Our vulnerability detection goes beyond just Microsoft product updates and includes other third party applications, as we review reporting of identified vulnerabilities regularly to ensure that any vulnerabilities are remediated.

WEBPAY & WEB TIME ENVIRONMENT DMZS

Our Web Pay and Web Time environments are hosted in segregated network segments. Control points only allow necessary outbound and inbound network traffic to reduce the impact of a compromise resulting from web application vulnerabilities; as all connections to our web servers require an HTTPS connection using TLS encryption.



paylocity

Paylocity (NASDAQ: PCTY) is a leading provider of cloud-based payroll and human capital management software solutions. Our comprehensive and easy-to-use solutions enable our clients to manage their workforces more effectively. Our multi-tenant software platform is highly configurable and includes a unified suite of payroll and HCM applications, such as time and labor tracking, benefits and talent management. Paylocity's solutions help drive strategic human capital decision-making and improve employee engagement by enhancing the human resource, payroll and finance capabilities of our clients.

www.paylocity.com